invGUARD

Cyberattack prevention system

INOVENTICA TECHNOLOGIES

CONTENTS

invGUARD

Cyberattack prevention system

What is invGUARD?

invGUARD monitors real-time traffic flow in the network, for DDoS attack detection and mitigation to prevent adverse impact to the network, data centres, customers or services.

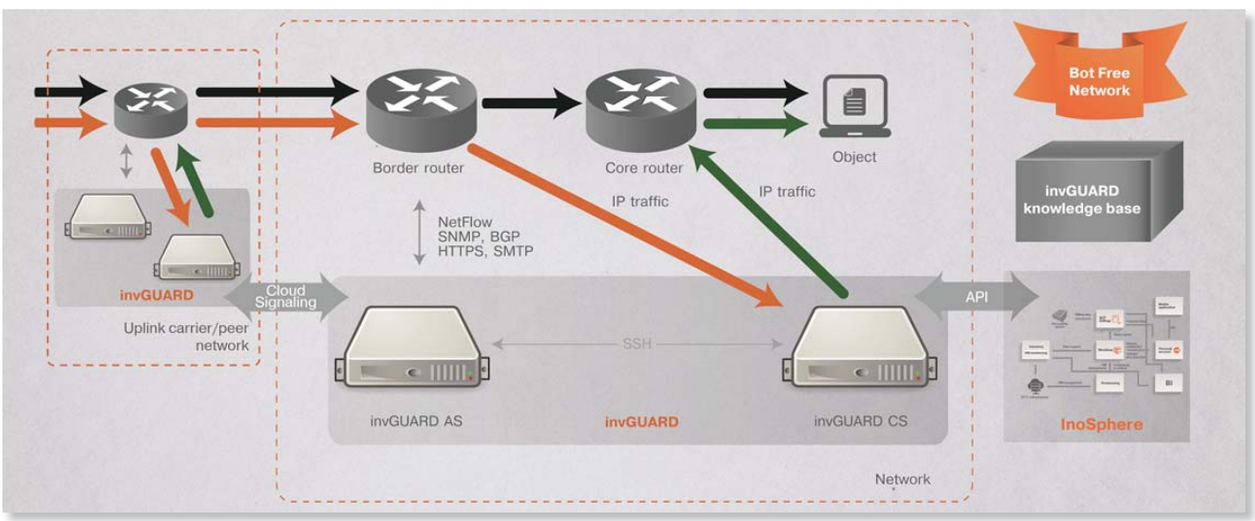
invGUARD offers:

- network visibility up to 5 Tbits with hundreds of routers
- real-time cyberattack detection and mitigation
- high-speed traffic cleaning & filtering up to 200 Gbits
- quality control of traffic flow to services, customers, uplinks and peers
- managed services for customers
- low cost of ownership

FUNCTIONALITY

- Collects and aggregates NetFlow data, SNMP and BGP updates from the network.
- Analyses traffic by customised views with TCP/IP stack and BGP information.
- Detects anomalous behavior of managed objects and signatureless malicious impacts to the network.
- Detects DDoS attacks such as ICMP flood, TCP SYN flood, TCP Connection flood, UDP flood and more than 100 other types of attacks.
- Generates more than 250 different real-time and historic reports.
- Mitigates attacks with BGP updates: Blackhole and FlowSpec.
- Cleans traffic from worms, zombies, botnets and other types of malicious impacts.
- Activates countermeasures to prevent malicious impacts: connections, amount of data, etc.
- Integrates with customer's security monitoring centers via SNMP.
- Network routers supported: Juniper, Cisco, Huawei, HPE, H3C, Extreme etc.
- Multi-language interface.

SYSTEM ARCHITECTURE



TECHNOLOGIES

- Traffic flow analysis: NetFlow v5, v9 and IPFIX, NetStream v5 and v9, sFlow
- Router status and data: SNMP v2c and v3
- Routings table and traffic flow management: BGP v4
- OS: Linux (Red Hat, CentOS or similar)
- x86 CPU: server hardware agnostic
- KVM virtual machine support for invGuard AS
- MySQL Database
- Apache web server
- Rapid traffic cleaning: special high-speed or Intel DPDK supported network cards

PERFORMANCE

- Up to 5 Tbits traffic analysis for cyberattack prevention
- 100+ routers in single management interface
- 20000+ managed objects
- Multi-vendors environment: Juniper, HPE, H3C, Cisco, Huawei, Alcatel, Exterme, etc.
- 250+ customized views of traffic and objects
- 100+ types of detectable cyberattacks
- 10000+ threats per day
- 80- hours for on-site deployment

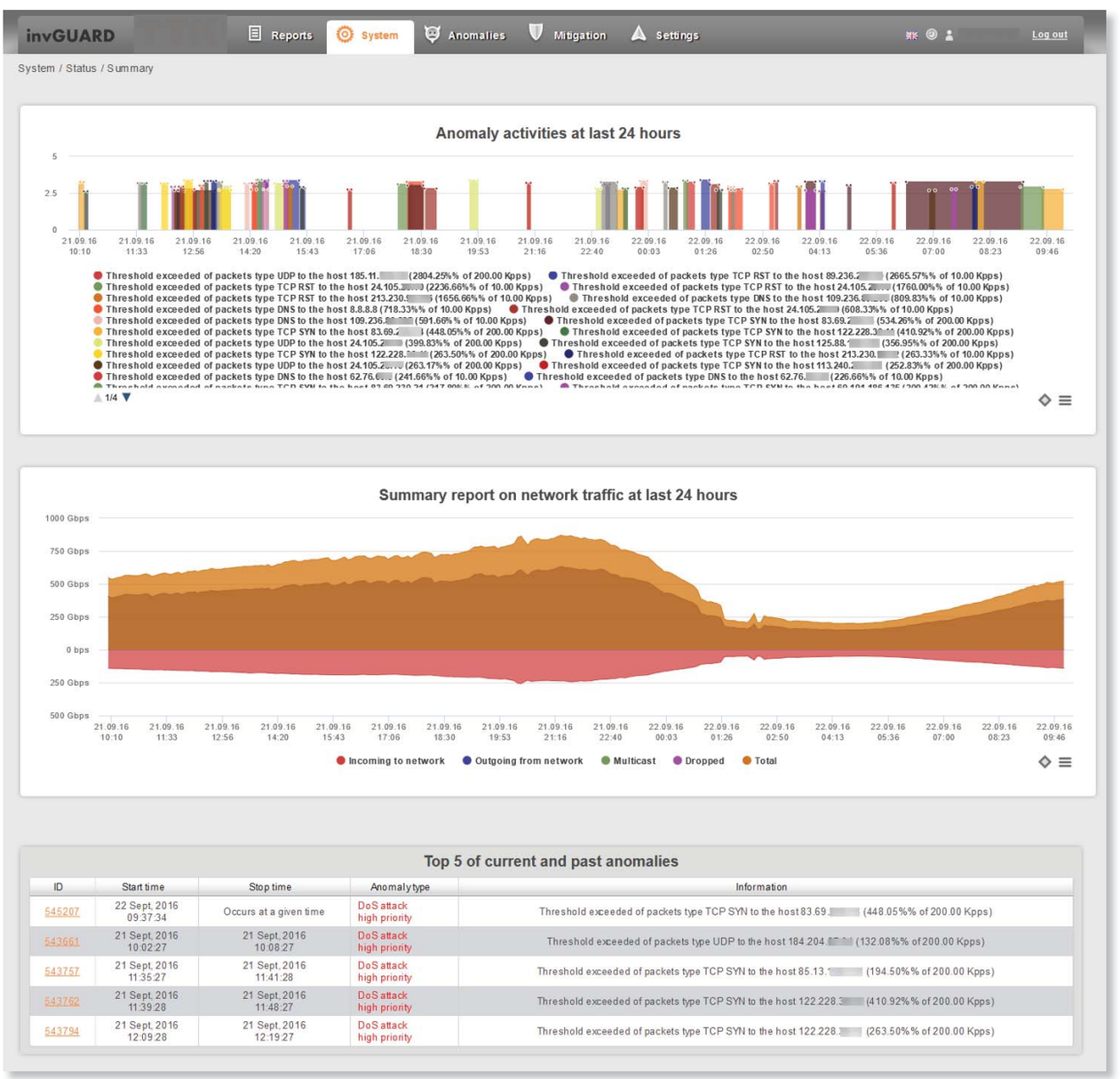
invGUARD

Cyberattack prevention system

invGUARD AS – ANALYZER

invGUARD AS is the main invGuard system component:

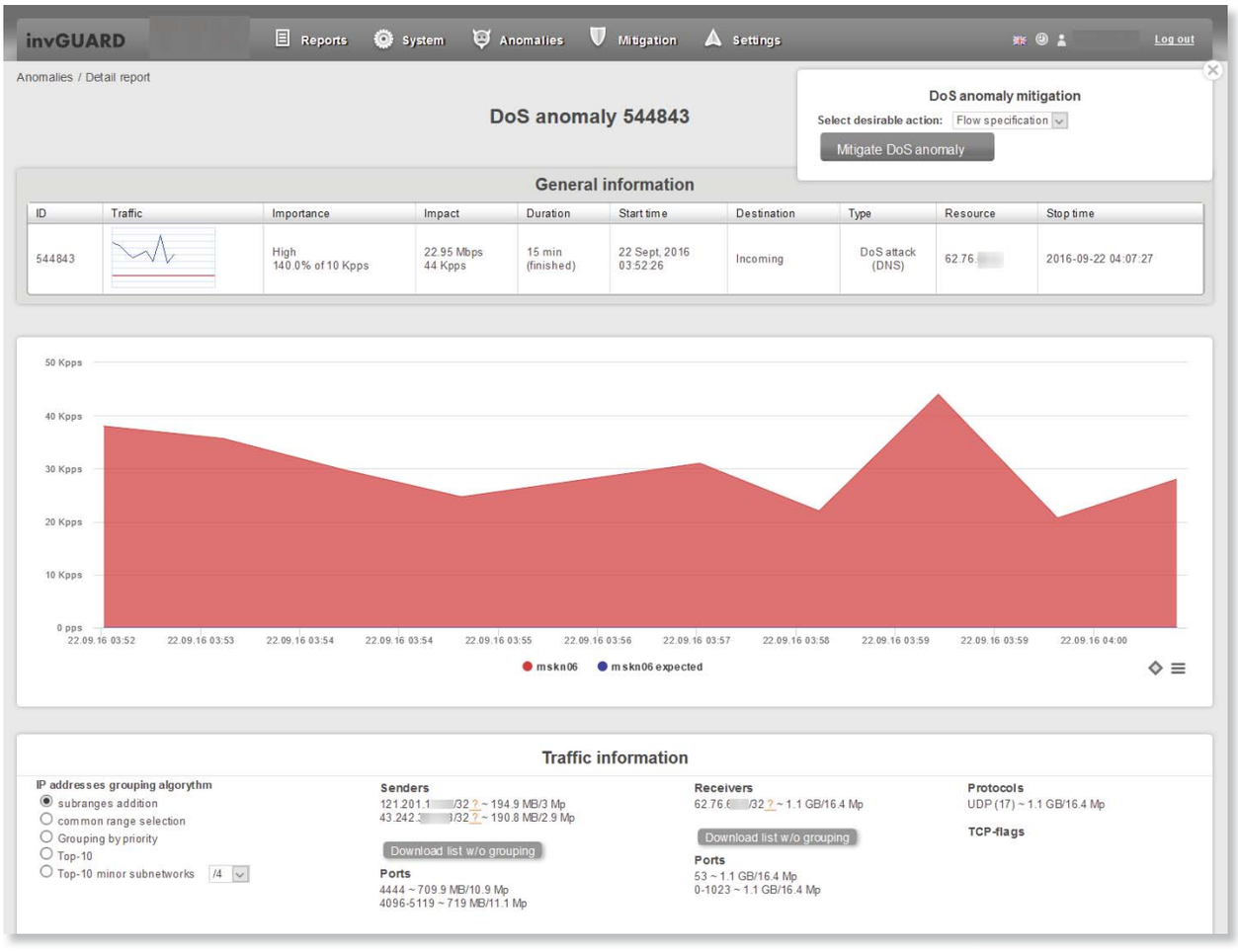
- collects, aggregates, analyses and stores network data from routers via NetFlow, SNMP and BGP;
- detects network traffic anomalies, DDoS and other types of network attacks;
- generates detailed network traffic reports.



Network status page

invGUARD AS – BLOCKING ATTACKS ON ROUTERS

- Block traffic: BGP Blackhole routing
- Dynamic filtering on routers (BGP flowspec): source IP, destination IP, protocols, ports, flags, packet size, fragmentation, DSCP
- ACL filtering: ports, source IP, destination IP, flags, protocols
- Black and white lists filtering
- Traffic shaping



Anomaly detection and BGP FlowSpec selected action

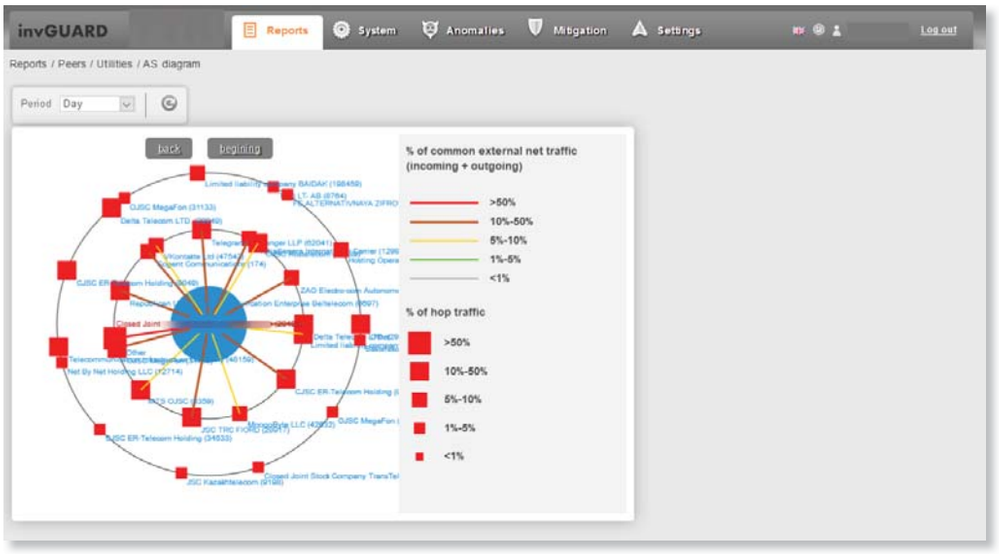
invGUARD

Cyberattack prevention system

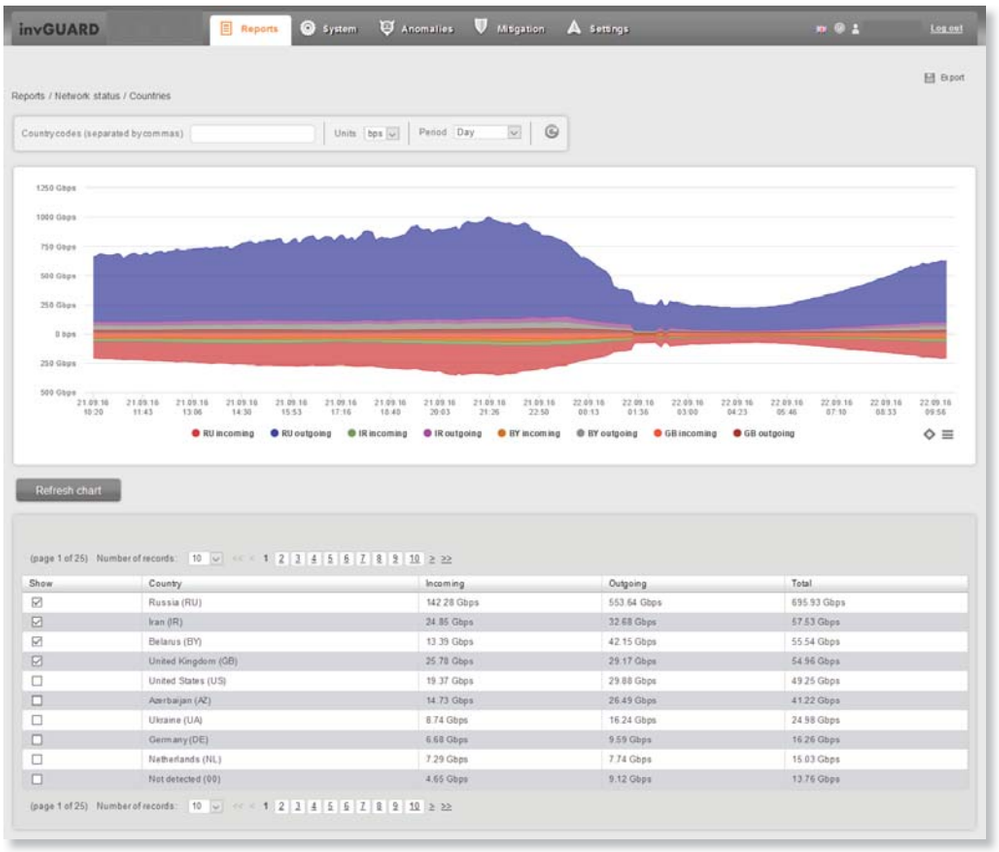
TOOLS FOR DECISION MAKING

invGUARD AS is a tool for answering the following questions:

- what traffic is coming from and going to the network;
- what routes traffic takes;
- what interfaces and routers are used;
- who are the top talkers on the network or objects;



Peers and uplinks

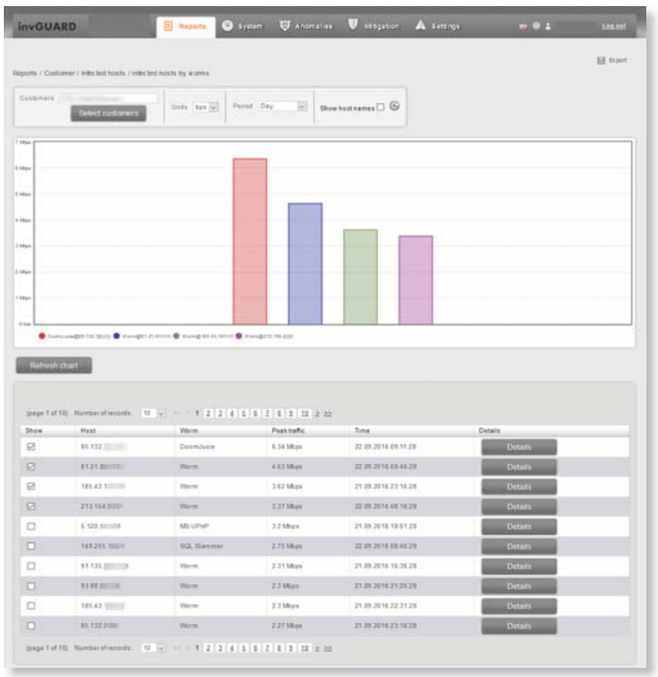


Geo IP functionality

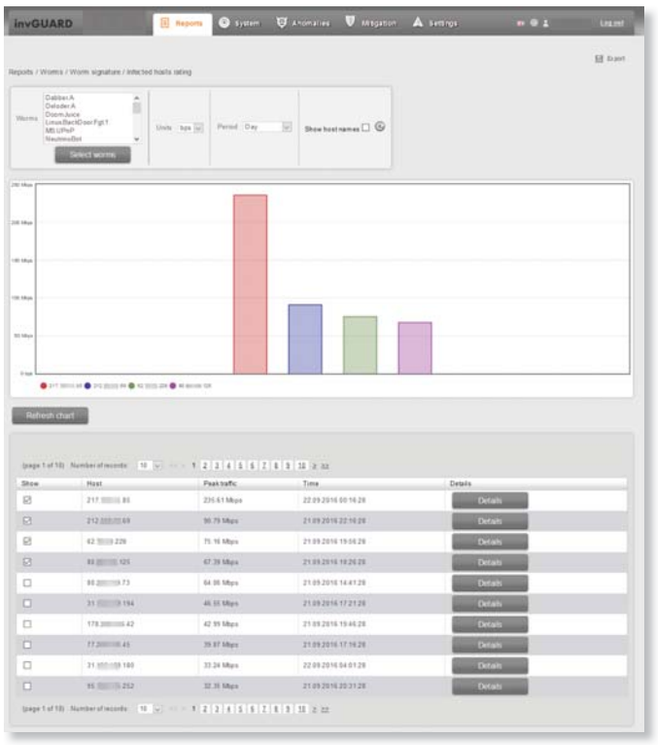
SECURITY

invGUARD detects:

- infected hosts in the network;
- hosts that could soon become the targets of attacks;
- hosts of botnets in the networks;
- hosts of botnets in the networks that are talking with management centers.



Peers and uplinks



Botnets in the networks

invGUARD

Cyberattack prevention system

invGUARD AS SPECIFICATION (PER APPLIANCE):

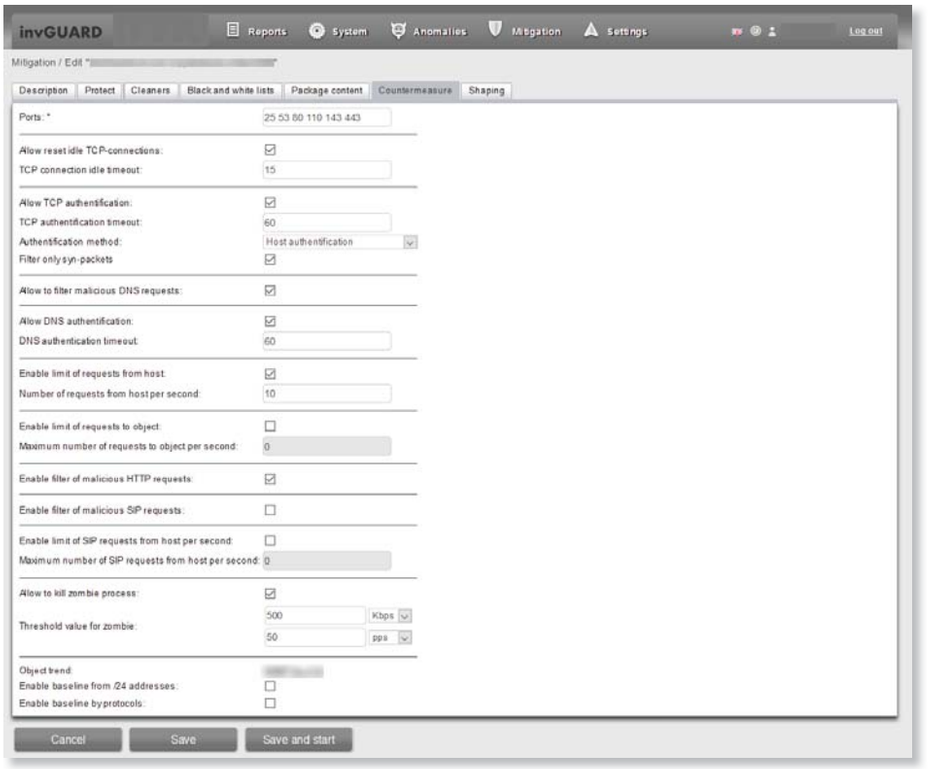
- Analysis and cyberattack detection up to 5 Tbits with 100000 NetFlow rps rate;
- BGP: up to 100 routers with 650,000 routing records;
- Detailed statistics on interrelations in controlled network infrastructure allows the user to manage network resources efficiently and quickly detect network bottlenecks;
- Management API for creating/updating managed objects, detection thresholds, activating automitigation, reporting (traffic statistics, anomalies, mitigation tasks)
- Notification center: email by SMTP, SNMP traps and syslog;
- Web interface for management (administrators, security engineers);
- Web interface for customer's susbscribers (personal accounts).

invGUARD CS – CLEANER

invGUARD CS accurately cleans traffic.
To redirect traffic from its normal flow for cleaning, invGuard AS sends a BGP update to the routers – and attack traffic flows directly to invGuard CS.

invGUARD CS:

- assembles traffic by sessions to distinguish malicious impacts;
- uses attack database and countermeasures settings to mark traffic packets;
- drops illegitimate traffic;
- passes clean traffic to its destination.



invGuard CS mitigation settings

invGUARD CS – ATTACK MITIGATION

- SYN authorisation: TCP packet blocking, connection authorisation, host authorisation
- DNS authorisation: fake source address packet blocking
- Black and white lists
- Global filter: filter settings on signature basis
- Zombie detection: filtering by number of connections, number of connection requests, traffic volume
- TCP sessions hanging: identification and reset of hanging sessions
- TCP session assembling: right sequence of TCP fragments from source to destination
- Attack auto-mitigation: filtering activation on basis of tasks from invGUARD AS
- Shaping: decreasing traffic according to thresholds
- Detailed statistics on attack mitigation to invGuard AS
- If needed, Raw traffic storage may be activated during active tasks

invGUARD CS SPECIFICATION (PER APPLIANCE):

- invGUARD CS: traffic cleaning up to 20 Gbits
- invGUARD CS-01: traffic cleaning up to 1 Gbits
- Attack mitigation at application level (HTTP, DNS, SIP,…)
- Automatic, semi-automatic and manual attack mitigation
- Precision filtering settings supported

invGUARD IMPLEMENTATION VALUES

1. Cost-efficient solution for cyberattack detection and prevention (DoS/DDoS attacks, signatureless malicious impacts)

invGUARD saves investments - there is no need to upgrade existing network equipment while using open formats for traffic statistics – SNMP and NetFlow.

Best practice is to use the BGP protocol for routing data and for traffic routing – Blackhole, FlowSpec and nexthop traffic diversion – invGUARD has it all.

invGUARD detects anomalies and impacts as a behavior of managed object traffic. There is no need to subscribe to any malware signatures database.

2. Risk reduction of denial-of-service attack to managed objects (web sites, e-shops, media, etc.)

invGUARD detects traffic anomalies, DoS/DDoS attacks and signatureless malicious impacts and informs network management employees or security experts in real time to minimise the impacts on managed objects and help them to stay permanently online.

invGUARD filters traffic for black/white list, protocol misuse and malicious impacts to prevent DoS/DDoS attacks on managed objects.

3. Efficient tool for traffic analysis and network infrastructure optimization

invGUARD offers whole-network traffic visibility up to 5 Tbits with hundreds of routers: 250+ customised views of traffic by protocols, applications, BGP attributes, managed objects, interfaces, QoS, routing information, prefixes, countries.

invGUARD helps to make reasonable decisions on optimization of network traffic flows, routes and network infrastructure.

4. Easy integration with existing network management platforms via SNMP (HP OV, IBM Tivoli, Zabbix, Nagios, etc.)

invGUARD can be easily integrated with monitoring systems and network management platforms via the SNMP protocol. The system sends traps and has SNMP registered OID enterprise.44937.1.1 for SNMP requests from external systems.
Additionally, invGUARD has a SYSLOG event tracking tool to export or import security events to external systems.

5. Extra security via multi-level protection (Cloud Signalling)

invGUARD supports multi-node solutions with Cloud Signalling functionality to build network border-like protection from high volume DoS/DDoS attacks.

invGUARD is a tool for efficient multi-level protection.

6. SLA monitoring for managed object access

invGUARD provides 250+ reports that helps to build SLA monitoring of accessibility to managed objects and exports them to network management team and security experts. Reports provide information about traffic profiles and thresholds, downtimes, etc.

7. Efficient tool for managing telco services expenses

invGUARD generates uplink/peer traffic reports and gives the ability to identify the most dangerous (sources of most attacks) and the most secure (sources of no attacks) providers. Provides tools for managing network equipment interface utilization for underload and overload.

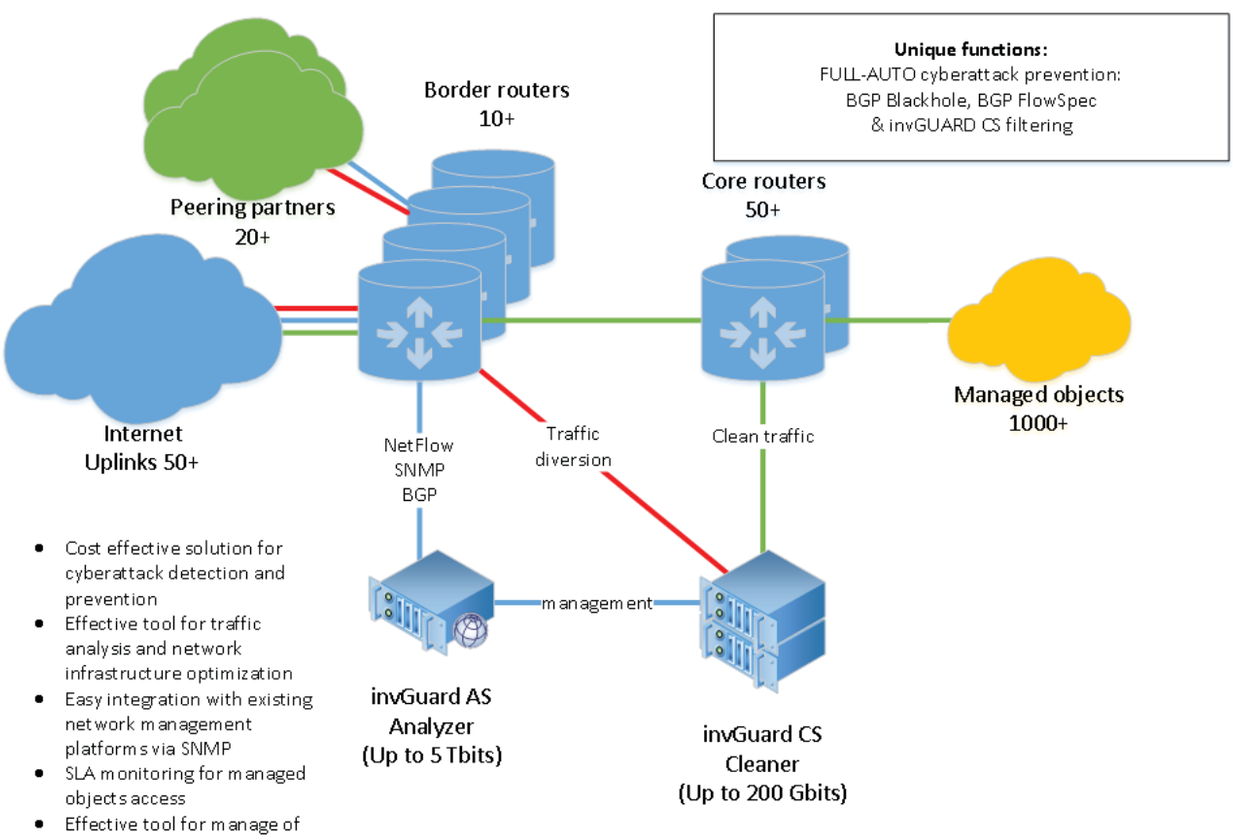
8. Extra revenue source from DoS/DDoS prevention services for B2B/B2C (easy integration with InoSphere Cloud Services management platform)

invGUARD has open integration API and has preconfigured sets of options for providing DoS/DDoS prevention services with the shortest warmup on the market. It makes invGUARD a new revenue source for these services.

InoSphere is a management platform for providing cloud services for B2B/B2C in auto mode. InoSphere is a platform with built-in invGUARD integration for ready-to-go DoS/DDoS prevention services and ability to supply paid services to customers.

invGUARD MARKETPLACE

Telecom carriers

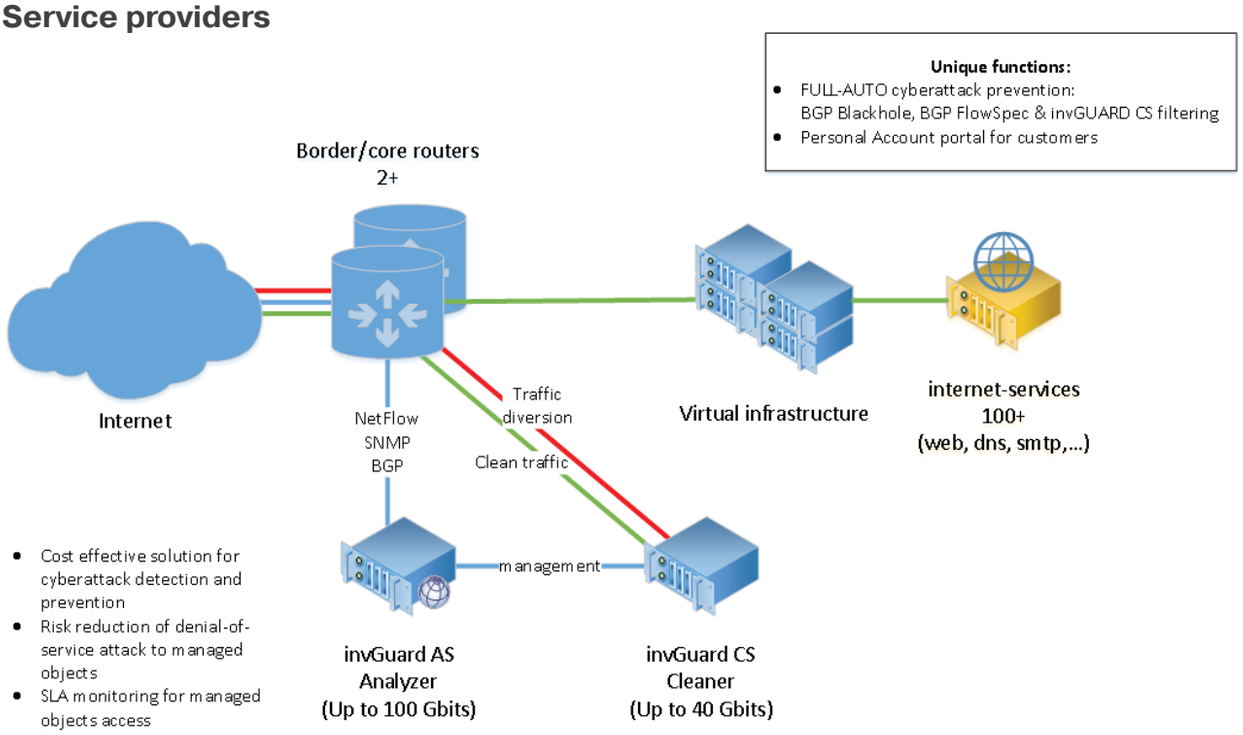


- Cost effective solution for cyberattack detection and prevention
- Effective tool for traffic analysis and network infrastructure optimization
- Easy integration with existing network management platforms via SNMP
- SLA monitoring for managed objects access
- Effective tool for manage of telco services expenses

invGUARD

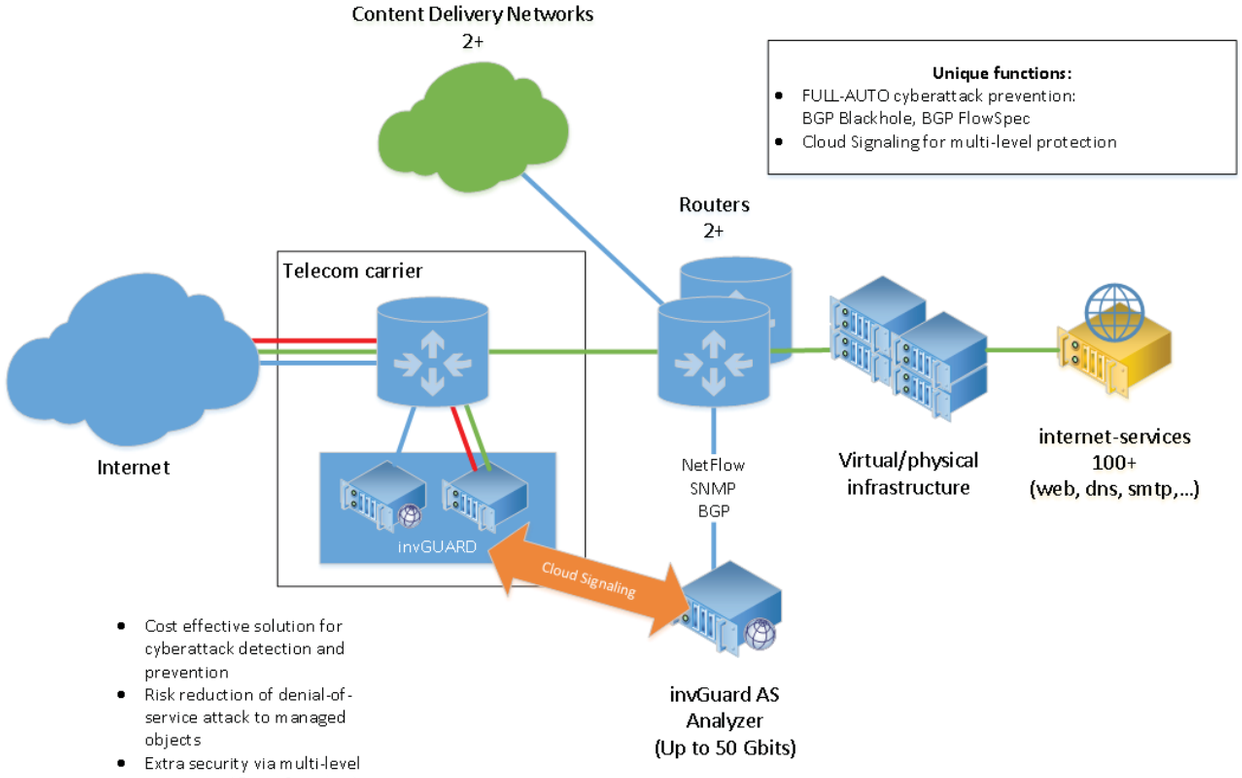
Cyberattack prevention system

Service providers



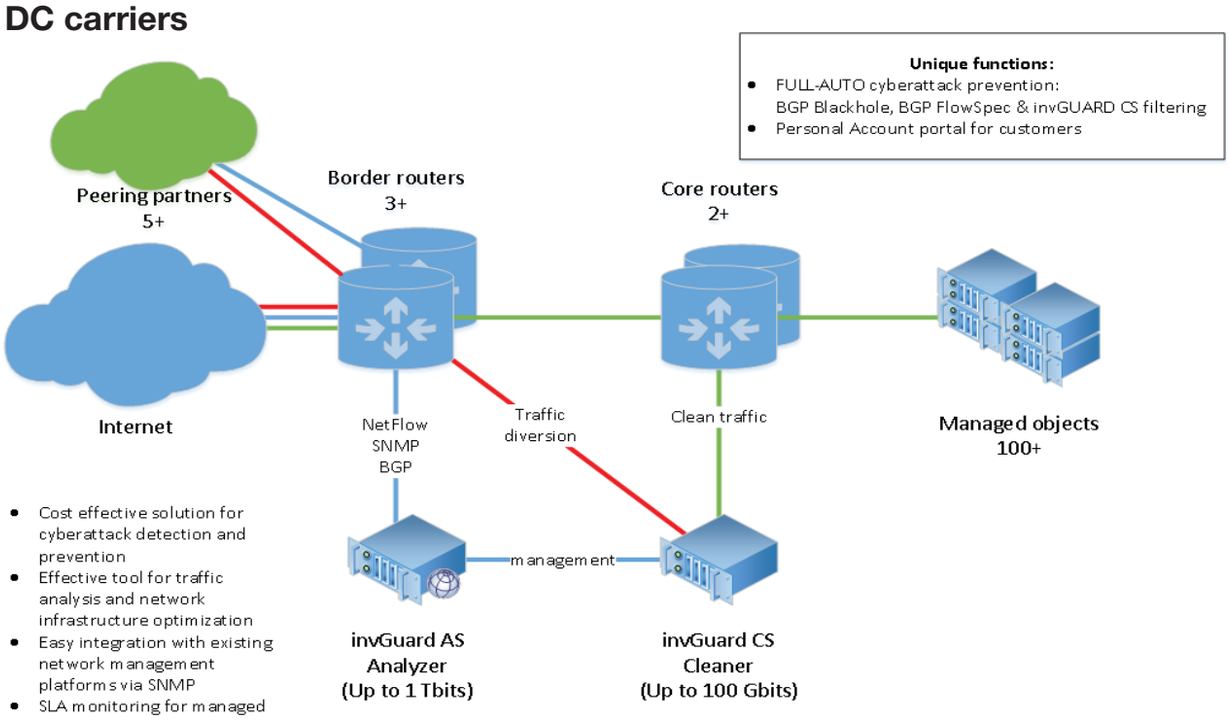
- Cost effective solution for cyberattack detection and prevention
- Risk reduction of denial-of-service attack to managed objects
- SLA monitoring for managed objects access
- Effective tool for manage of telco services expenses

Media companies



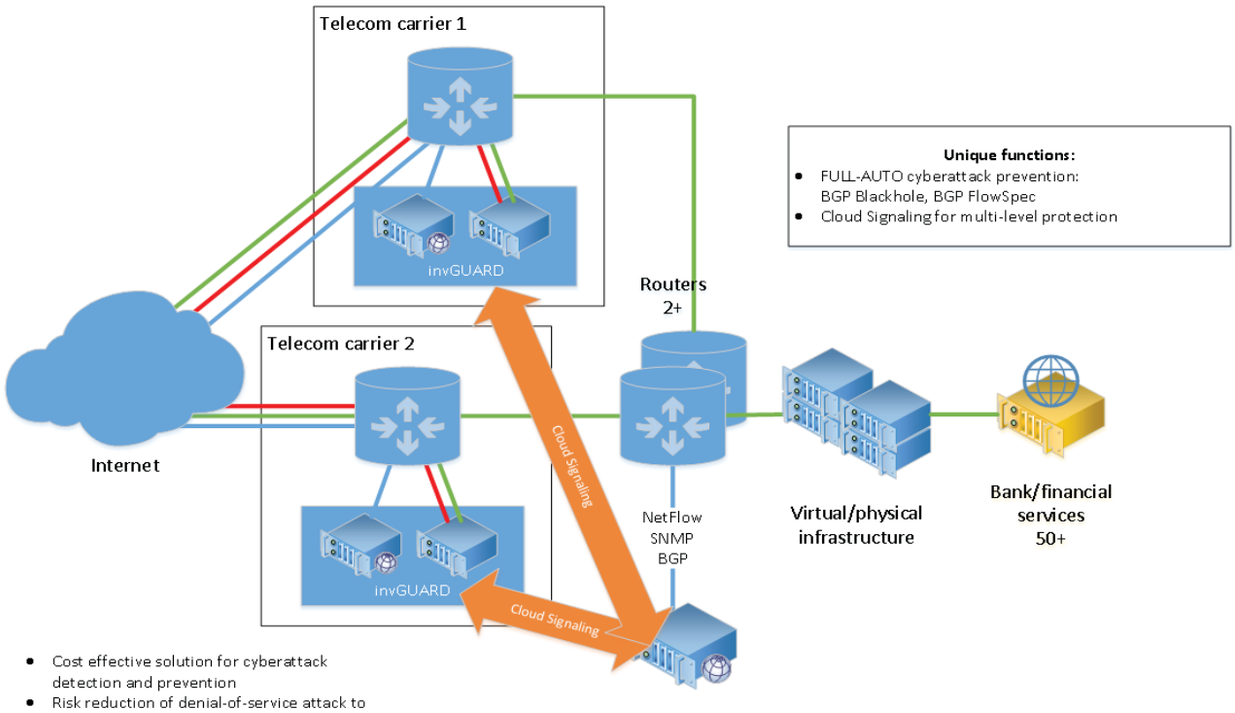
- Cost effective solution for cyberattack detection and prevention
- Risk reduction of denial-of-service attack to managed objects
- Extra security via multi-level protection (Cloud Signaling)
- SLA monitoring for managed objects access
- Effective tool for manage of telco services expenses

DC carriers



- Cost effective solution for cyberattack detection and prevention
- Effective tool for traffic analysis and network infrastructure optimization
- Easy integration with existing network management platforms via SNMP
- SLA monitoring for managed objects access
- Effective tool for manage of telco services expenses

Banks and financial institutes

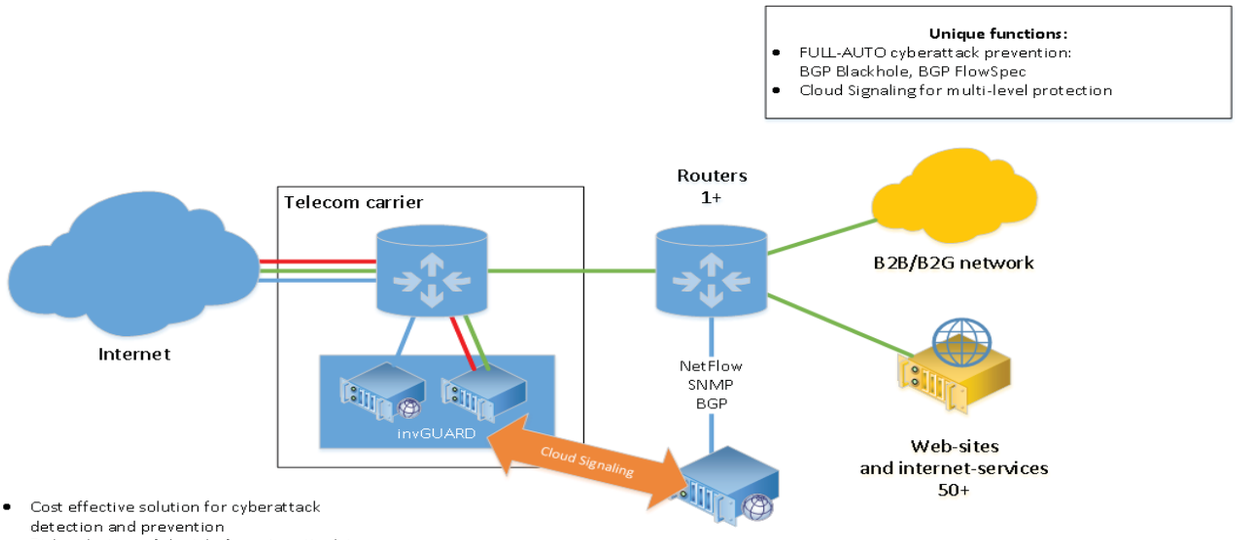


- Cost effective solution for cyberattack detection and prevention
- Risk reduction of denial-of-service attack to managed objects
- Easy integration with existing network management platforms via SNMP
- Extra security via multi-level protection (Cloud Signaling)
- SLA monitoring for managed objects access
- Effective tool for manage of telco services expenses

invGUARD

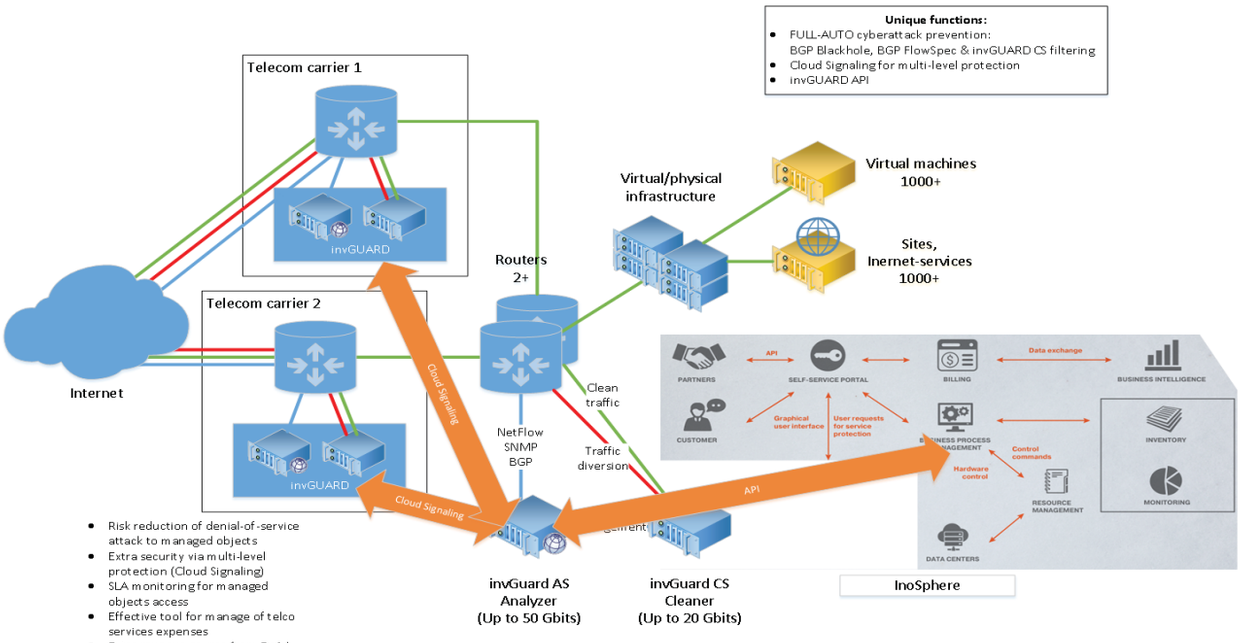
Cyberattack prevention system

B2B and B2G with substantial own IT infrastructure



- Cost effective solution for cyberattack detection and prevention
- Risk reduction of denial-of-service attack to managed objects
- Easy integration with existing network management platforms via SNMP
- Extra security via multi-level protection (Cloud Signaling)
- SLA monitoring for managed objects access
- Effective tool for manage of telco services expenses

Cyberattack prevention for mass-market cloud/hosting providers



- Risk reduction of denial-of-service attack to managed objects
- Extra security via multi-level protection (Cloud Signaling)
- SLA monitoring for managed objects access
- Effective tool for manage of telco services expenses
- Extra revenue source from DoS/DDoS prevention services for B2B/B2C (easy integration with InoSphere Cloud Services management platform)

TECHNICAL SPECIFICATIONS

NETFLOW COLLECTOR

invGUARD collects traffic statistics:

- NetFlow v5
- NetFlow v9
- NetFlow v10
- NetStream v5 & v9 for Huawei routers with SNMP correlation table
- IPFIX
- sFlow

NetFlow settings: IP address of source, port, sampling rate

SNMP COMMUNICATION

invGUARD collects interfaces info by SNMP:

- routers interfaces – ifIndex, description, speed, IP addresses
- traffic statistics
- router CPU data
- router RAM data

SNMP-traps for external monitoring systems:

- invGUARD is designed to integrate with external monitoring systems to send cyberattack detection events through an SNMP-trap mechanism.
- External monitoring system can request invGUARD's extra cyberattack detection information through SNMP v2c with specific invGUARD SNMP OID (enterprise.44937.1.1).
- invGUARD supports external monitoring systems like Zabbix, Nagios, etc.

SNMP settings: version, IP address, community (v2/v2c), login/password (v3)

TRAFFIC ROUTING

- BGP announces for changing routing table:
  - Blackhole
  - NextHop
  - FlowSpec
- Dynamic routing with GRE tunnels on invGUARD CS

BGP settings: router IP, router ID, local and remote ASN, md5 key

BGP-PEERING

- iBGP-peering
- iBGP-peering with mirroring routers
- iBGP-peering with route server
- BGP-table from other router
- eBGP-peering

ANOMALY DETECTION

- BGP traps
- BGP instability
- BGP phishing
- BGP lost of connection
- NetFlow drops
- SNMP lost of connection
- DoS & DDoS attacks
- Thresholds of traffic amount
- Thresholds of interface load
- Thresholds of managed object traffic
- Dark IP traffic

BOT DETECTION

- Detection of bot activity
- Alerts on thresholds by bot activity

CYBERATTACK DETECTION

- TCP SYN Flood
- TCP RST Flood
- TCP Flood
- HTTP Flood
- DNS Request Flood
- DNS Amplification
- NTP Amplification
- SSDP Amplification
- FTP Flood
- Incorrect SIP
- UDP Flood (UDP based services: SNMP, Radius, NTP, IPSec over UDP and others)
- ICMP Echo Request/Reply Flood

FINGERPRINTS

invGUARD has cyberattack fingerpints to be built by customers or updated from central database:

- User can create fingerprint via invGUARD interface
- Fingerprint updates from central database

INTERFACES CONFIGURATION

- list of interfaces
- change of the name, description or speed
- change of classification (instead of automatic)
- thresholds by interface

INTERFACES AUTOCONFIGURATION

- Autoconfiguration rule management: every interface change on routers is detected and invGUARD runs rules to match interface type.
- Rules define regular expressions (regexp) for interfaces descriptions to match the type of interfaces
- Rules define types of interface (internal, external, ignored or other)

MANAGED OBJECTS

- Types: customer, profile, peer, worm
- Traffic fingerprint:
  - Boolean expression
  - ASPath regexp
  - CIDR blocks
  - CIDR groups
  - BGP community
  - Interfaces
  - Peer ASN
  - Local ASN or SubAS
- Object traffic thresholds by detectors or by traffic behavior
- Settings for detection and notification
- Settings for mitigation: automatic/manual, mitigation templates

SELF-SECURITY

- Secure channels among invGUARD subsystems
- Access control
- User authorization management
- Historical reports of user's access
- NetFlow phishing detection

REPORTS

Every report has functionality to configure the report period (day, week, month, year or custom) and to export reports to text, xml or pdf format (simply by clicking the 'Export' button and selecting format).

1. **Summary by any period**
2. **Summary with active anomalies**
3. **Current and previous anomalies with custom filter (importance, managed object, router, thresholds, etc.)**
4. **Detailed system status**
5. **Summary for routers & router dashboard**
6. **Summary for interfaces**
7. **Summary and details for BGP (routing table,**
8. **NetFlow/SNMP comparing**
9. **Reports by managed objects:**
   - a. Summary
   - b. By protocols: ICMP, TCP, UDP
   - c. By BGP attributes: all ASN, Origin ASN, ASN peer, AS path, ASxAS, communities, Next hops, prefixes
   - d. By routers
   - e. By interfaces
   - f. By other managed objects (customer, peer, profile)
   - g. Multicase
   - h. QoS
     - i. ToS
     - ii. DTRM
     - iii. IP Precedence
   - i. By packet size
   - j. By countries
10. **Reports by worms and bots:**
    - a. Activity per object or IP
    - b. Infected hosts (inside or outside network)
11. **Reports by invGUARD CS**
    - a. Traffic filtering
    - b. Statistics:
    - i. By protocols
    - ii. By HTTP: URLs
    - iii. By DNS: domains
    - iv. By SIP: caller numbers
12. **Anomaly reports:**
    - a. Current anomalies
    - b. Detailed anomaly:
    - i. Impact
    - ii. Detailed IPs: senders/receivers
    - iii. Ports
    - iv. Countries
    - v. ASNs
    - vi. Packet sizes
    - vii. Routers and interfaces
    - c. Historical anomalies

invGUARD API

The **API** (application programming interface) is used for invGUARD management from external systems through HTTPS with JSON format messages packed with MessagePack.

The **API can be used for:**

- creating, changing and viewing managed objects;
- cyberattack detection settings management;
- requesting current and historical detected cyberattack information;
- cyberattack mitigation settings management;
- requesting current and historical cyberattack mitigations status and statistics;
- requesting current and historical managed object traffic information data.

invGUARD + InoSphere

invGUARD is designed for quick and easy integration with inoSphere Cloud Services management platform to provide additional security services for inoSphere users.

inoSphere users have free of charge access to traffic statistics for every ordered service for each IP address used.

Additional security services include cyberattack detection and cyberattack prevention. inoSphere has customizable invGUARD security settings for every inoSphere service (such as VM or hosting). Additional security services have different tariffs: per month or per hour.

inoSphere users can easily manage additional security services provided by invGUARD and choose the tariff they like through the inoSphere Personal Account web-site.

invGUARD FOR EXTERNAL MONITORING SYSTEMS VIA SNMP

invGUARD is designed to integrate with external monitoring systems to send cyberattack detection events through the SNMP-trap mechanism.

External monitoring system can request invGUARD for extra cyberattack detection information through SNMP v2c with specific invGUARD SNMP OID (enterprise.44937.1.1).

invGUARD supports external monitoring systems like Zabbix, Nagios, etc.

invGUARD CLOUD SIGNALLING

invGUARD Cloud Signalling provides functionality for “cloud” traffic cleaning from cyberattacks, black/white lists filtering, shaping and protocol misuse.

invGUARD Cloud Signaling can be used on invGUARD AS system to connect to the “Cloud” formed by the Cloud Signaling service provided by other invGUARD customers. . In this case invGUARD customers who don’t have invGUARD CS system installed can use the “cloud” for attack mitigation.

invGUARD systems use a standardised protocol called invGUARD Cloud Signalling for inter-communication and transfer attack mitigation tasks and statistics without any private data being stored in the invGUARD system.

The invGUARD Cloud Signalling “Customer” role can be assigned to any invGUARD AS system to provide additional capabilities for attack mitigation with functionality of traffic filtering on an invGUARD system with “Provider” role without needing to install invGUARD CS.

The invGUARD Cloud Signalling “Provider” role can be assigned to a full invGUARD installation (invGUARD AS and invGUARD CS systems) to connect invGUARD Cloud Signalling “Customer” systems and to provide attack mitigation services on the “Provider” system for:

- Black/white lists filtering
- TCP protocol authorization
- TCP connection control and limit
- HTTP, DNS, SIP protocols RFC check
- Number of concurrent requests from/to managed object or host
- Packet payload regex check
- Baseline control
- Zombie detection
- Traffic shaping

invGUARD ROAD MAP

2H 2017	1H 2018	2H 2018
• BI tools for cyberattack analysis • IPv6 collector • IPv6 analysis & cyberattack detection • IPv6 traffic reporting • BGP for IPv6 • IPv6 BGP Blackhole & FlowSpec mitigation • Anti-virus vendor partnerships and integrations	• IPv6 cyberattack mitigation & traffic filtering • New methods for 100Gbps+ cyberattack mitigation • API for integrations with third-party security solutions	• Neural networks for precision cyberattack detection and mitigation • Fully-automatic cyberattack detection and mitigation

SUPPORT AND MAINTENANCE

- Free system updates within the Global Updates Programme
- Technical support 24x7 or 8x5 time schedule
- New custom reports - from 2 weeks
- Integration with network management platforms – from 1 day

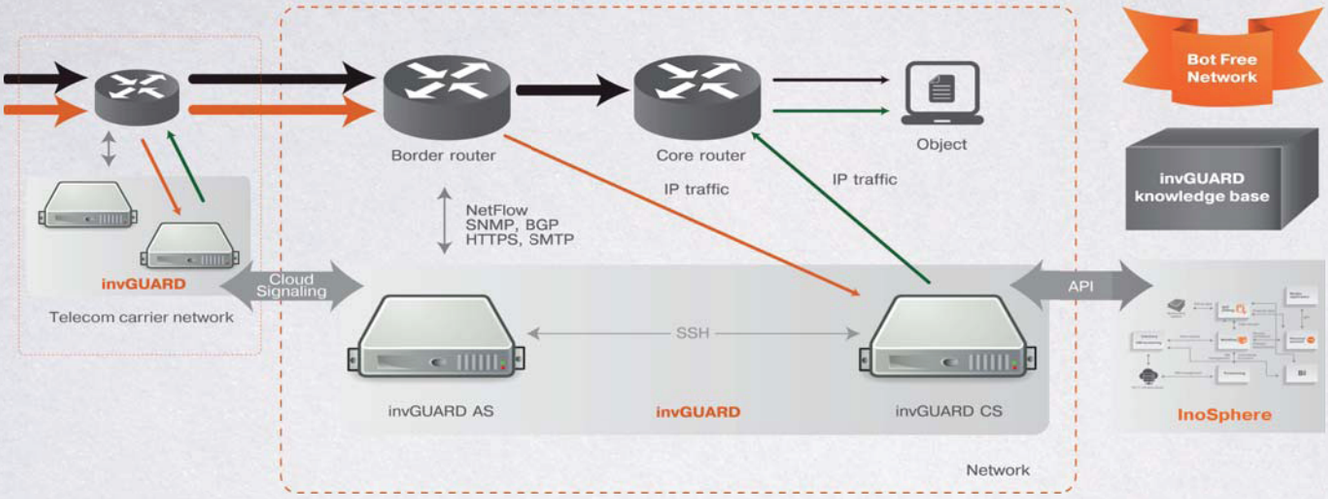
IMPLEMENTATION

Implementation takes 2 weeks for the typical network: 3-5 routers, 100 Gbits traffic flow.

On-site and off-site implementation

Employee's training by invGUARD experts

SYSTEM ARCHITECTURE

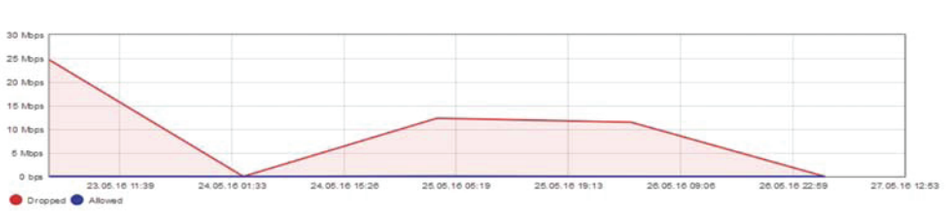


DETECTED DOS ATTACKS AND ANOMALIES

521446		High 104.7% of 6 Gbps	13.4 Gbps 1.27 Mpps	16 min (finished)	28 July 2016 16:15:38	Incoming	DoS attack (Amount of traffic, bits per second)
521445		High 83.4% of 700 Kpps	13.39 Gbps 1.24 Mpps	16 min (finished)	28 July 2016 16:15:37	Incoming	DoS attack (UDP flood)
521451		Medium 85.0% of 361.82 Mbps	668.48 Mbps 136.33 Kpps	6 min (finished)	28 July 2016 16:16:36	Incoming	DoS attack (Excess traffic to profile)
520928		Medium 83.8% of 78.6 Kpps	1.07 Gbps 187.15 Kpps	2 h 24 min (finished)	28 July 2016 13:34:35	Incoming	DoS attack (Excess traffic to profile)
521161		High 3000.0% of 200 Kbps	48 Mbps 4 Kpps	18 min (finished)	28 July 2016 14:47:35	Incoming	DoS attack (Excess traffic to profile)
521142		High 58.8% of 150 Kpps	146.22 Mbps 281.15 Kpps	17 min (finished)	28 July 2016 14:41:35	Outgoing	DoS attack (DNS)
521110		Medium 88.8% of 10.88 Kpps	55.67 Mbps 24.17 Kpps	7 min (finished)	28 July 2016 14:31:35	Incoming	DoS attack (Excess traffic to profile)

invGUARD TRAFFIC CLEANING

Name	[redacted]
Task ID	2
Cleaner	Cleaner 1
Prefixes	[redacted]143.35/32
Start time	27 May 2016 12:53:08
Duration	[redacted] min
Status	Stopped



Traffic

Period	Incoming	Allowed	Dropped	% Allowed
Last minute	0 bps/0 pps	0 bps/0 pps	0 bps/0 pps	0%
All time	6.98 Mbps/7.93 Kpps	4.04 Mbps/4.38 Kpps	3.64 Mbps/5.02 Kpps	58%

Global exception list

	Period	Allowed	% Allowed	Dropped	% Dropped
	Last minute	0 bps/0 pps	0%	0 bps/0 pps	0%
⊞	All time	5.99 Mbps/6.87 Kpps	86%	987.65 Kbps/1.05 Kpps	14%

inoventica.eu

facebook.com/inoventica vk.com/inoventica twitter.com/inoventica instagram.com/inoventica